Digital Forensics Tools/Vendor တွေရဲ့ တစ်ကယ့်အမှန်တရားများ

Aung Zaw Myo (ThirdEye)
www.forensicsmyanmar.com

Digital Forensics Tools/Vendor တွေရဲ့ တစ်ကယ့်အမှန်တရားများ

အခုလက်ရှိမှာ Mobile Phone , Computer စတဲ့ Digital ပစ္စည်းထုတ်လုပ်တဲ့ Vendor တွေများ လာသလို Digital Product တွေရဲ့လုံခြုံရေးကလဲမြင့်လာပါတယ်။ ဒါကြောင့်အချို့ Forensics Vendor တွေက Lock , Encryption ဖြည်တာနဲ့ပတ်သတ်ပြီး ပွင့်လင်းစွာပြောဆိုတာ ဖော်ပြတာတွေမှာ ကန့်သတ်ချက်ရှိ လာပါ တယ်။

တစ်နေ့ထက်တစ်နေ့ အပြိုင်အဆိုင်ထုတ်လုပ်ကျတဲ့ Digital Product တွေ Security , Encryption Feature တွေကြောင့် Forensics Vendor တွေကလဲ ထွက်သမျှ နည်းပညာ နောက်ကို လိုက်ပြီး Update ဖြစ်အောင်ပြုလုပ်ရပါတယ်။ ဒါပေမဲ့ နောက်ဆုံးပေါ် Digital Products, Security တွေအားလုံးကို Forensics Vendor တွေက Support မပေးနိုင်ပါဘူး။ ဥပမာ ဒီနေ့ IOS 15 ထွက်ရင် နောက်နေ့မှာ Forensics Vendor ကနေ အဲဒီအတွက် ချက်ချင်း Support မပြုလုပ်နိုင်ပါဘူး။ အချိန်ကာလ တစ်ခုအထိစောင့်ရပါတယ်။

Apple က အာနည်းချက်ပြင်ပြီး Security Update လုပ်ခိုင်းတဲ့နောက်ပိုင်း အဲဒီ Version မှာရှိတဲ့ အားနည်းချက်မရှိတော့ရင် Forensics Vendor/ Tool က အရင်ကလုပ်နိုင်သလို မလုပ်နိုင်တော့ပါဘူး။ နောက်ပြီးရင် Forensics Vendor က ဈေးကွက်ထဲမှာ လူအသုံးများဆုံး Product နဲ့ File Format အတွက်သာ အဓိက Support ပြုလုပ်မှာဖြစ်ပါတယ်။ လူသုံးနည်းတဲ့ Brand , File Format ကို Support ပြုလုပ်မှာ မဟုတ်ပါဘူး။

Digital Forensics Tools တွေက Digital Device တွေထဲက Data တွေကိုထုတ်ယူပြီး Analysis ပြုလုပ်တာဖြစ်ပါတယ်။ Digital Forensics Tools တွေမှာသုံးတဲ့ Algorithms တွေက များစွာသော Digital Device တွေအပေါ်မှာပြုလုပ်ရတာဖြစ်တာကြောင့် False Positives Or False Negatives တွေရှိပါတယ်။ ဥပမာ အနေနဲ့ မြင်သာသိသာအောင် Data တွေကိုဖော်ပြတဲ့နေရာ။ Log တွေကိုဖော်ပြတဲ့နေရာမှာ ဖြစ်ပါတယ်။ ဒီလိုဖြစ်တာတွေကို Forensics Vendor တွေကထုတ်ပြောမှာမဟုတ်ပါဘူး။ False Positives Or False Negatives တွေကြောင့် Tools တစ်ခုထဲကို အားကိုးပြီး စစ်ဆေးသူ၊ Tools ကိုပဲသုံးတတ်ပြီး Knowledge အားနည်းတဲ့စစ်ဆေးသူတွေအတွက် အဓိက အခက်ခဲ စိန်ခေါ်မှုဖြစ်လာပါတယ်။

အခုအချိန်မှာ လူတွေက နည်းပညာကို ထိတွေ့ဆက်ဆံလာတာများလာတဲ့အတွက် Privacy, Data Protection, Encryption, Security တွေကိုလဲ ထုတ်လုပ်သူတွေဘက်က အဆင်မြင့်လာပါတယ်။ ဒါကြောင့် Forensics Vendor တွေအနေနဲ့ Data ကို Device တွေထဲကနေ ထုတ်ယူတဲ့နေရာမှာ အခက်အခဲအကန့် အသတ်တွေရှိလာပါတယ်။ ဥပမာ အရင် ၁၀ နှစ်လောက်တုန်းက ဖုန်းတွေမှာ မြန်မာစာမြင်ရဖို့နဲ့ မြန်မာလိုရေးလို့ရအောင်ဆိုပြီး Jailbreak, Root ပြုလုပ်ခဲ့ပေမဲ့ အခုအချိန်မှာ ဘယ်သူမှ ပြုလုပ်စရာမလို တော့ပါဘူး။ ဒါကြောင့် Jailbreak, Root လုပ်ထားတဲ့

ဖုန်းထဲကနေ Data ရယူနိုင်တာနဲ့ Jailbreak , Root မလုပ်တဲ့ ဖုန်းကနေ Data ရယူတဲ့နေရာ မှာ အများကြီး ကွာခြားသွားပါတယ်။

တစ်ကယ်လို့ Mobile Phone တစ်လုံးက Lock အနေအထားနဲ့စစ်ဆေးရမယ်ဆိုရင် Forensics Tools မှာ အကန့်အသတ်ရှိသွားပါပြီ။ Tools ကနေ Support ပေးတဲ့ ***Brand, Model, OS Version, Firmware , Chipset Version*** မဟုတ်ရင် Phone ထဲကနေ Data မရယူနိုင်တော့ပါဘူး။ ရယူဖို့ခက်ခဲသွားပါပြီ။

Forensics Vendor တွေကလဲ Compatibility Lists တွေကို မပြည့်မစုံပေးထားတတ်သလို အချို့အကြောင်းအရာတွေကို Secret အနေနဲ့ မထုတ်ဖော်ပါဘူး။ ဥပမာ UFED ဆိုရင် စစ်ဆေးတဲ့နေရာမှာ အခက်ခဲရှိတာနဲ့ Premium Support အကူအညီယူနိုင်ပြီး ပိုက်ဆံပေးရပါတယ်။ ဒါမျိုးနဲ့ သူ့ Tools ရဲ့ လုပ်နိုင် ဆောင်စွမ်းကို အခြားပြိုင်ဘက်တွေ Mobile Phone Vendor တွေမသိတောင် ထိန်းသိမ်းထားပါတယ်။ Premium Support မှာနဲ့ တစ်ကယ့် Tools မှာပါတာက ကွာခြားပါတယ်။

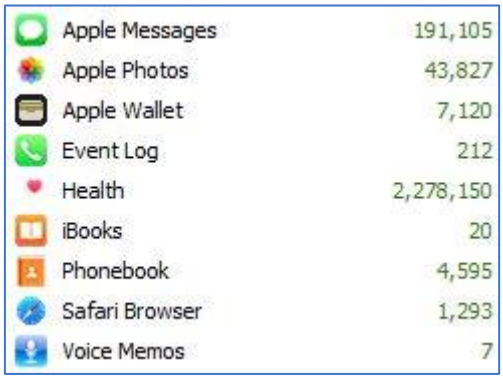
Digital Forensics Vendor တိုင်ပြောနေကျ ကြော်ငြာနေကျစကားလုံးတွေရှိပါတယ်။ Marketing အရသုံးနေကျစကားလုံးတွေပဲဖြစ်ပါတယ်။

- *Company A, the global leader in Digital Intelligence Solution*
- *Company B, a global leader in forensic technology for mobile device investigations…*
- *Company C is a global leader in digital forensics technology*
- *Company D, a global leader in digital forensics for law enforcement*
- *Company E, the industry's leading provider of digital forensic investigation technology…*
- *Company F is a world leader in forensic technology…*
- *Company G is a global leader in digital forensics software.*
- *Company H is a leading provider of mobile device digital forensics.*

အချို့ Vendor တွေကျတော့ Product ရဲ့ လုပ်ဆောင်နိုင်စွမ်းနဲ့ အားနည်းချက်အားသာချက်ကို အခြားပြိုင်ဘက် တွေသိသွား မှာစိုးတာရော၊ အားနည်းချက်ကို တစ်ဖက်က ပြင်သွားမှာစိုးတာရောနဲ့ ဝယ်ယူတဲ့သူကို NDA ထိုးခိုင်းပါတယ်။ ဥပမာ IOS Version (….)မှာ အားနည်ချက်ရှိတယ် အဲဒီအားနည်းချက်ကို အခွင့်ကောင်းယူပြီး ဘယ်လို Data တွေကိုရယူနိုင်တယ်ဆိုတာကို Apple ဘက်နေသိသွားရင် သူတို့ဘက်ကနေ ချက်ချင်း အားနည်းချက်ကိုပြင်သွားနိုင်ပါတယ်။ နောက်တစ်ခုကတော့ Vendor တွေအဓိကထားတာက ဝယ်တဲ့သူ အသုံးပြုတဲ့သူကို နှစ်ရှည်ဝယ်ယူ သုံးအောင်

ဖြစ်ပါတယ်။ Digital Forensics Vendor တွေကတစ်ကယ်တော့ ဈေးကွက်မှာလဲ ရွေးချယ်စရာ နည်းပါးပါတယ် ဒါကြောင့် သူတို့ Product ကို သုံးတာကြာလာတာနဲ့အမျှ ဝယ်တဲ့သူ အသုံးပြု သူဘက်က သူတို့ချမှတ်ထားတဲ့ စည်းကမ်းတွေ နဲ့ ကန့်သတ်ချက်တွေကို ကျင့်သားရလာမှာကို သိနေ လို့ဖြစ်ပါတယ်။ ဆိုလိုတာက ဒါကိုသုံးရင်တော့ ဒီလောက်ပဲရနိုင်မယ်။ ဒီလောက်အထိ ပဲရနိုင်တယ်ဆို ပြီး အသုံးပြုသူဘက်နေ ကျင့်သားရသွားတာကိုပြောချင်တာပါ။ Bait-And-Switch Tactics ကိုအသုံးပြုလိုပါပဲ။ အွန်လိုင်းကနေရောင်းတဲ့ ပစ္စည်းကို ပုံစံလေး Specification လေးကိုသဘော ကျလို့မှာတယ် ဒါပေမဲ့ Delivery နဲ့ ကိုယ့်ဆီကို ရောက်လာတဲ့အချိန်မှာ အွန်းလိုင်းမှာပြတဲ့ပုံစံနဲ့ တစ်လွဲစီဖြစ်နေတာမျိုးပေါ့။

ဘယ်လိုအကြောင်းတွေပဲရှိရှိ Support လုပ်တဲ့ Device And Methods တွေ၊ Data ကိုထုတ်ယူတဲ့နည်းလမ်းတွေ၊ Recovery ပြုလုပ်တဲ့နည်းလမ်းတွေနဲ့ ကျန်တဲ့ ကန့်သတ်ချက်တွေကို တစ်ခါတစ်လေမှာ ရောင်းသူဘက်ကထုတ်ဖော်မပြောဆိုပါဘူး။ ဈေးကွက်ထဲမှာတွေ့နေကျ စကား လုံးတွေဖြစ်တဲ့ Advanced strategy 1” or “Supersonic brute-force ဆိုတာတွေ ရဲ့နောက် ကွယ်မှာ Password Attack ပြုလုပ်ဖို့အတွက် လိုအပ်တဲ့ Hardware Requirements တွေ ကန့်သတ် ချက်တွေ ကိုပြောဆိုမှာမဟုတ်ပါဘူး။ Crack ပြုလုပ်နိုင်တဲ့ Speed ကိုလဲပြောမှာမဟုတ်ပါဘူး။ Knowledge နည်းတဲ့ ဝယ်သူကလဲ ဒီ Password Crack Tools ကိုသုံးလိုက်တာနဲ့ ရုပ်ရှင်ထဲကလို Enter နှိပ်ရုံနဲ့ Password ရလာတယ်လို့ ထင်နေနိုင်ပါတယ်။ လိုင်စင်ဝယ်ပြီးတဲ့ အချိန်ရောက် မှ လိုအပ်တာတွေကို ဝယ်သူဘက်ကနေ လိုက်ရှာရ ဖြည့်ရတာ တွေရှိလာပါမယ်။ ဒါမှမဟုတ်လဲ ကန့်သတ်ချက်တွေ အသုံးပြုနည်းတွေ လိုအပ်ချက်တွေကို သိဖို့အတွက် Tools လိုင်စင် ထက်ဈေးကြီးတဲ့ သူတို့ဘက် ကနေဖွင့်တဲ့ သင်တန်းတွေကို တက်ရပါလိမ့်မယ်။ တစ်ကယ်တန်း တိကျသေချာတဲ့ အချက်အလက်နဲ့ သဲလွန်စ မရှိရင် Password Crack ပြုလုပ်တာက မလွယ်ကူပါဘူး။



အပေါ်ကပုံတွေမှာဆိုရင် Apple Wallet Artifacts တွေ 7120 ရှိကြောင်းပြပါမယ်။ တစ်ကယ်တန်းပြတဲ့အခါမှာ အသုံးဝင်တာ 288 ခုပဲရှိပါတယ်။ ဘယ်လိုပဲဖြစ်ဖြစ် Artifacts မှန်သမျှက အသုံးဝင်နိုင်တယ်ဆိုပေမဲ့ အချက်အလက်တွေက အသုံးပြုတဲ့ Tools အလိုက်ဖော်ပြတဲ့ အရေအတွက် မတူတာတွေ အချက်အလက်ဖောင်းပွတာတွေရှိ ပါတယ်။ Vendor တွေကလဲ အချက်အလက်ပိုရ ကြောင်းပြချင်တဲ့အတွက် မလိုအပ်တာတွေပါ Artifacts ထဲမှာထည့်ပြတာတွေရှိပါတယ်။

တစ်ခါတစ်ရံမှာ Vendor တွေကနေ Android Lock Bypass , IOS Lock Bypass, All User's Deleted Data Can Recovery ဆိုပြီး လွန်လွန်ကျူးကျူးကြော်ငြာတာတွေတွေ့ရပါမယ်။ တစ်ကယ်တန်းစမ်းသပ်သုံးကြည့်ရရင် Limitation တွေကို သေချာမေးကြည့်ရင် Brand တစ်ခုမှာမှ အားနည်းချက်ရှိတဲ့ Model တစ်ခု နှစ်ခုလောက်ကိုပဲ ပြုလုပ်နိုင်ပါတယ်။ ဒါတောင်မှ အဲဒီ Model တွေမှာ ပြောတဲ့အတိုင်း ရနိုင်ဖို့အတွက် ကန့်သတ်ချက်တွေရှိပါတယ်။ Product မှာ conditions တွေကောင်းကောင်းရေးထားပေမဲ့ Supported Models, Operating System, Application Versions အလိုက် ကန့်သတ်ချက်ကို ပြည့်ပြည့်စုံစုံဖော်ပြထားမှာ မဟုတ်ပါဘူး။ Premium Version, Premium Support တွေမှာလဲ တိတိကျကျဖော်ပြတာ ပြောပြတာနည်းပါးပါတယ်။

လိုင်စင်နဲ့ပတ်သတ်ပြီးတော့ လိုင်စင်ကုန်ရင် ဘယ်လိုဖြစ်မယ် ဘယ်လို Function တွေဆက်ပြီး အသုံးပြုလို့ ရတယ်။ License Refund, License Penalty အကြောင်းကိုလဲ တိတိကျကျပြောဆိုတာမရှိပါ။ (တိတိကျကျ မမေးတာလဲ ပါပါတယ်။)

အတော်များများသော Digital Forensics Vendor တွေက Open-Source Code တွေကို ယူပြီး အသုံးပြုပါတယ်။ ဥပမာ checkra1n Jailbreak, Checkm8 Exploit ကိုအသုံးပြုပြီး Checkm8 Extraction နည်းလမ်းကို Forensics Vendor တော်တော်များများအသုံးပြုပါတယ်။ (Checkm8 Extraction ဆိုတာက IOS Bootloader အားနည်းချက်ကို အသုံးချပြီး Apple Phone ကို Device Firmware Upgrade (DFU Mode) ကိုပြောင်းပြီး IOS File System ကနေရမဲ့ Data နဲ့ IOS keychain ကိုရယူတာဖြစ်ပါတယ်။)

အနှစ်ချုပ်အနေနဲ့ DFIR Field မှာ တစ်ခုတည်းနဲ့ပြီး ဟိုဟာလဲ ဒီဟာလဲရတယ်ဆိုပြီး ပြည့်စုံတာ မရှိပါ။ ***No Single Software Solution.***

Vendor တွေက လွန်လွန်ကျူးကျူး Marketing သဘောအရ ပြောတတ် ကြေငြာတတ်ပါတယ်။ *ဒါကြောင့် လိုအပ်တွေ့ ကန့်သတ်ချက်တွေ့ အသေအချာမေးမြန်းရပါမယ်။*

Dig Deeper To Ensure The Best Outcomes.

REFERENCE

https://blog.elcomsoft.com/2023/06/what-forensic-vendors-dont-like-to-tell-their-customers-part-1/

https://blog.elcomsoft.com/2023/06/what-forensic-vendors-dont-like-to-tell-their-customers-part-2/

Aung Zaw Myo (Third Eye)

www.forensicsmyanmar.com